ABSTRACT OF THE DISCLOSURE

An apparatus and method for performing a modular operation S=AB mod N, the apparatus arranged such that the constant J0, which is ordinarily required in order to complete the operation, is not required to be explicitly computed, thus simplifying and speeding up the operation.